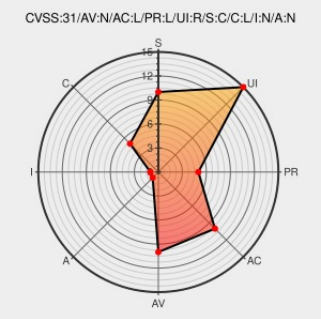
CVE-2020-5270

Published on: 04/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-5270 - advisory for GHSA-375w-q56h-h7qc

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Prestashop from Prestashop contain the following vulnerability:

In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is an open redirection when using back parameter. The impacts can be many, and vary from the theft of information and credentials to the redirection to malicious websites containing attacker-controlled content, which in some cases even cause XSS attacks. So even though an open redirection might sound harmless at first, the impacts of it can be severe should it be exploitable. The problem is fixed in 1.7.6.5

CVE-2020-5270 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **PrestaShop** - **PrestaShop** version **>= 1.7.6.0, < 1.7.6.5**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Open redirection when using back parameter · Advisory · PrestaShop/PrestaShop · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/PrestaShop/PrestaShop/security/advisories/GHSA-375v h7qc
Merge pull request from GHSA-375w-q56h-h7qc · PrestaShop/PrestaShop@cd2219d · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/PrestaShop/PrestaShop/commit/cd2219dca49965ae8421bb5a53fc301

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Prestashop	Prestashop	All	All	All	All
Application	Prestashop	Prestashop	All	All	All	All

cpe:2.3:a:prestashop:prestashop:*:*:*:*:*:*:*:*:

cpe:2.3:a:prestashop:prestashop:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→